Cryptography

17^{th} February 2006

Definition 1. A *cryptosystem* is a system which modifies a message in such a way that it becomes unintelligible to anyone but the intended recipient. The process used in carrying this out is called *encryption*. A message thus encrypted is called *ciphertext*. The process by which a ciphertext is turned back into plaintext is called *decryption*. The art and science of encrypting messages is called *encryption*, whereas that of decrypting ciphertext without the key is called *cryptanalysis*. Both cryptography and cryptanalysis make up a branch of mathematics called *cryptology*. Let m be a plaintext message, also denoted by p, $e(\cdot)$ the *encryption*, $d(m)$ the *decryption*, c an encrypted string, also known as *cipher*, *ciphertext*, or *cryptogram*, and k a *key*, that is a set of parameters. Then $d(e(m)) = m$ and $c = e(m, k)$. The range of all possible values of the key is called the *keyspace*.

§

Definition 2. There are two kinds of key-based algorithms, namely symmetric and public-key algorithms. *Symmetric* algorithms use the same key for both encryption and decryption. It is also known as *secret-key*, *single-key*, or *one-key* algorithms. There are two kinds of symmetric algorithms, stream and block ciphers. *Stream* algorithms work on a single bit at a time while *block* algorithms work on a group of bits. *Public-key* algorithms use different keys for encryption and decryption. The *encryption key* is called the *public key*, while the *decryption key* the *private key*. Encryption using public key is denoted by $e_k(p) = c$, decryption using the corresponding private key by $d_k(c) = p$. On the other hand, encryption using private key and decryption using public key, as in the case of digital signatures, are denoted respectively as $e_{k_d}(\cdot)$ and $d_{k_e}(\cdot)$.

§

Definition 3. An attempted cryptanalysis is called an *attack*. A successful attack is called a *method*. Assuming the encryption algorithm is known, there are six types of cryptanalysis attack, namely

a. *Cipher-text-only* attack. Here given $c_i = e_k(p_i)$, $i = 1, \dots, n$, we deduce either p_i, k, or an algorithm a that gives p_{n+1} from $c_{n+1} = e_k(p_{n+1})$, in other words $a : (c = e_k(p)) \mapsto p$.
b. *Known-plaintext* attack. Here given $c_i = e_k(p_i)$ and the corresponding p_i we deduce either k or $a : (c = e_k(p)) \mapsto p$.
c. *Chosen-plaintext* attack. Here choosing p_i we are given $c_i = e_k(p_i)$ and deduce either k or $a : (c = e_k(p)) \mapsto p$.
d. *Adaptive-chosen-plaintext* attack. Here choosing $p_i(c_{j<i})$ the choices of which are based on the results of previous encryption, we are provided with $c_i = e_k(p_i)$ and try to deduce either k or $a : (c = e_k(p)) \mapsto p$.
e. *Chosen-ciphertext* attack. Here choosing c_i we are given the corresponding $p_i = d_k(c_i)$ and try to deduce k.
f. *Chosen-key* attack. In this case you are given the key. So it is not in fact an attack, but rather only a decryption.

§

Definition 4. An algorithm that is unbreakable in practice is said to be *secure*. A secure algorithm can be *unconditionally secure* if there is not enough information to recover the plaintext no matter how much ciphertext one may have, or it can be *computationally secure*, or simply *strong*, if it cannot be broken with available resources. The amount of computing power and time required to recover the encryption key is called the *work factor*.

§

Definition 5. A *substitution cipher* is one in which each letter in the plaintext is replaced by another letter in the ciphertext. There are four types of substution cipher, namely

a. A *simple* substitution cipher. This is the case where the character replacements are one-to-one. In other words, $p^i \overset{one-one}{\longmapsto} c^i$.
b. A *homophonic* substitution cipher. Here the mapping of characters is one-to-many, that is $p^i \overset{one-many}{\longmapsto} c^i$.
c. A *polyalphabetic* substitution cipher. This is when there is a set of simple substitution ciphers for each character mapping, that is to say, $\left\{ p^i \overset{one-one}{\longmapsto} c^i \right\}$.

d. A *polygramme* substitution cipher. This is the case where substitution is done on blocks of characters instead of a single letter. Here $\mathbf{p}^i \overset{one-one}{\longmapsto} \mathbf{c}^i$.

§

Example 1. The *Caesar cipher* is a simple subsitution cipher in which each plaintext character is replaced by the character three to its right modulo 26, that is $c^i \leftarrow \big(p^i + 3\big)$ in $GF(26)$.

Example 2. *ROT13* is a simple encryption programme commonly found on UNIX systems. It has the procedure as shown in Algorithm 1.

given: c^i
if c^i is in $\{a, \ldots, m, A, \ldots, M\}$ **then**
  $c \leftarrow ((c + 13) \bmod 26)$
else
  $c \leftarrow ((c - 13) \bmod 26)$
endif

Definition 6. A *transposition cipher* is one in which the letters in the plaintext remain the same while their order is changed.

§

Definition 7. A *one-time pad* encryption algorithm is one which uses a non-repeating set of random key letters.

§

Bibliography

Bruce Schneier. *Applied cryptography.* John Wiley & Sons, 1994
Dominic Welsh. *Codes and cryptography.* Oxford, 1988